خيارات الأمان في الشبكات الاجتماعية

afte
مؤسسة حرية الفكر والتعبير
Association for Freedom of Thought and Expression

خيارات الأمان في الشبكات الاجتماعية

مؤسسة حرية الفكر والتعبير
4 شارع احمد باشا - الدور السادس - جاردن سيتي - القاهرة
تليفون/فاكس:27926281 (202)
البريد الإلكتروني: Info@afteegypt.org
الموقع الإلكتروني: www.afteegypt.org

إعداد

محمد الطاهر

منسق برنامج الحريات الرقمية بمؤسسة حرية الفكر والتعبير

تم إخراج هذه الورقة بالاعتماد برمجيات حرة، حزمة LibreOffice، وبرنامج Gimp، متصفح FireFox، نظام التشغيل Ubuntu

هذا الدليل

يقدم هذا الدليل شرح لخيارات الأمان التي توفرها الشبكات الاجتماعية، وقد قمنا باختيار أكثر الشبكات استخداما لتناولها (Facebook, Twitter) بالإضافة إلى خدمة البريد الإلكتروني (Gmail)، نظر لأنه يرتبط مع شبكة اجتماعية أخرى (Google +) وخدمات جوجل المتعددة مثل (Youtube)

فيسبوك

يتيح فيسبوك أكثر من خيار لحماية حسابك من الاطلاع على بياناتك الشخصية والسرقة . هذه الخيرات متاحة للاستخدام من خلال Security Settings . فيما يلي تفصيلا لهذه الخيارات:

ملاحظة قبل متابعة الشرح، تأكد من أنك قمت مسبقا بإضافة رقم هاتفك المحمول وتفعيله للاستخدام في فيسبوك، إذا لم تقم بفعل هذا يمكنك التوجه إلى التبويب Mobile الموجود في Account settings وإضافة رقم هاتفك، بعدها ستصلك رسالة تأكيد على رقمك لتنشيطه.

للدخول إلى إعدادات الأمن الخاصة بحسابك على فيسبوك، ادخل إلى Account Settings الموجودة بالقائمة إعدادات فيسبوك، ثم اختر التبويب Security Settings.

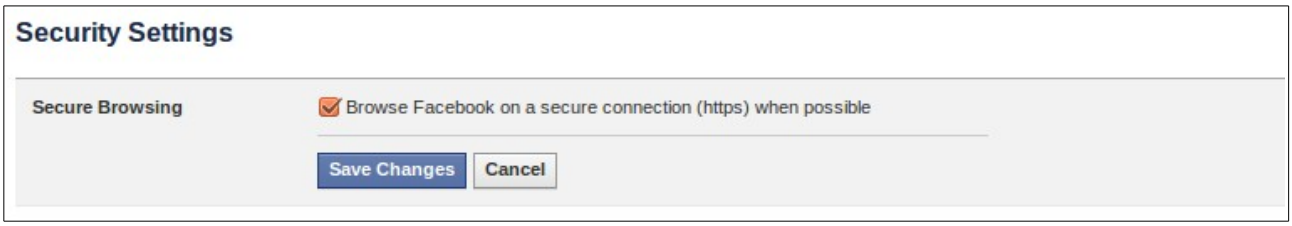
فيما يلي شرح خيارات الأمن المتاحة

نصائح عامة

- **قم** باختيار كلمة مرور صعبة، تحتوي على حروف صغيرة وكبيرة وأرقام ورموز، وحاول تغييرها على فترات لا تتجاوز ثلاثة أشهر.
- **احمي** بريدك الإلكتروني بقدر الإمكان، اختراق بريدك الإلكتروني يعني اختراق كافة حساباتك على الشبكات الاجتماعية
- **لا تقم** باستخدام أي تطبيق على فيسبوك دون أن يكون موثوق به ولا تقم بفتح الروابط غير الموثوق بها وتأكد دائما من أنك تستخدم بروتوكول https.
- **تجنب** حفظ كلمة السر في المتصفح، بل قم بإدخال كلمة المرور بكل مرة تقوم فيها باستخدام فيسبوك.
- **اهتم** بإعدادات الخصوصية وراجعها باستمرار ولاحظ أن فيسبوك يغير ويضيف الكثير من هذه الإعدادات كل فترة.
- **لا تقم** باستخدام حساب فيسبوك الخاص بك في المواقع، بل قم بالتسجيل العادي، وفي حالة، وجود مواقع ترتبط خدماتها بفيسبوك تأكد أنك تستخدم مواقع موثوق بها.

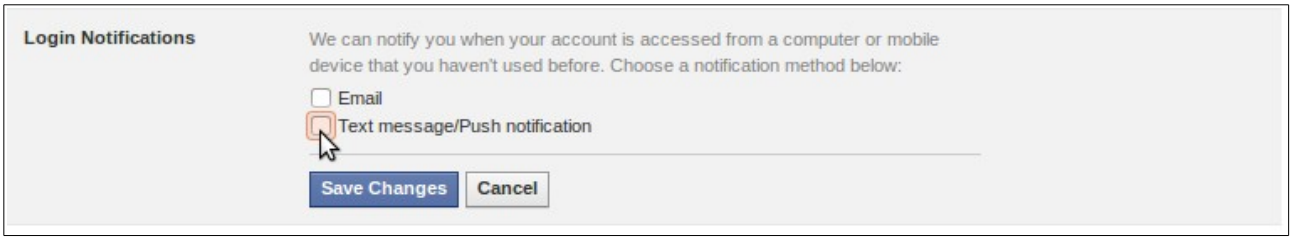
– Secure Browsing/التصفح الآمن

قم بتفعيل التصفح الآمن (https) هذا البروتوكول يوفر تشفير لتصفحك فيسبوك



– Login Notifications/إشعارات تسجيل الدخول

تفعيل هذا الخيار يعني أنه سيتم إعلامك في حالة تسجيل الدخول إلى حسابك من خلال (حاسب أو هاتف محمول أو جهاز لوحي) غير معروف (لم تستخدمه مسبقا) ويتوفر خيارين لإعلامك، عن طريق الرسائل النصية أو عن طريق البريد الإلكتروني.

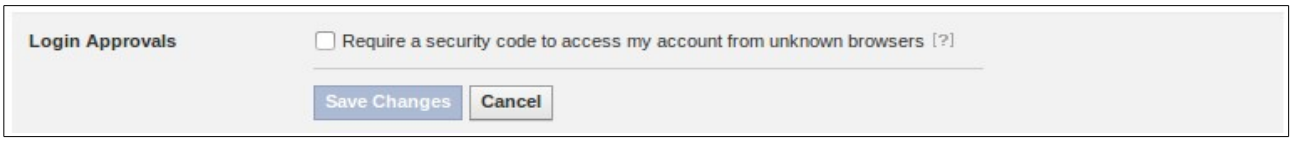


قم بتفعيل الخيارين Email و Text massage/Push notifications

– Login Approvals/الموافقات على تسجيل الدخول

ملاحظة هامه: يجب أن تكون وضعت مسبقا رقم هاتفك المحمول وقمت بتفعيلة.

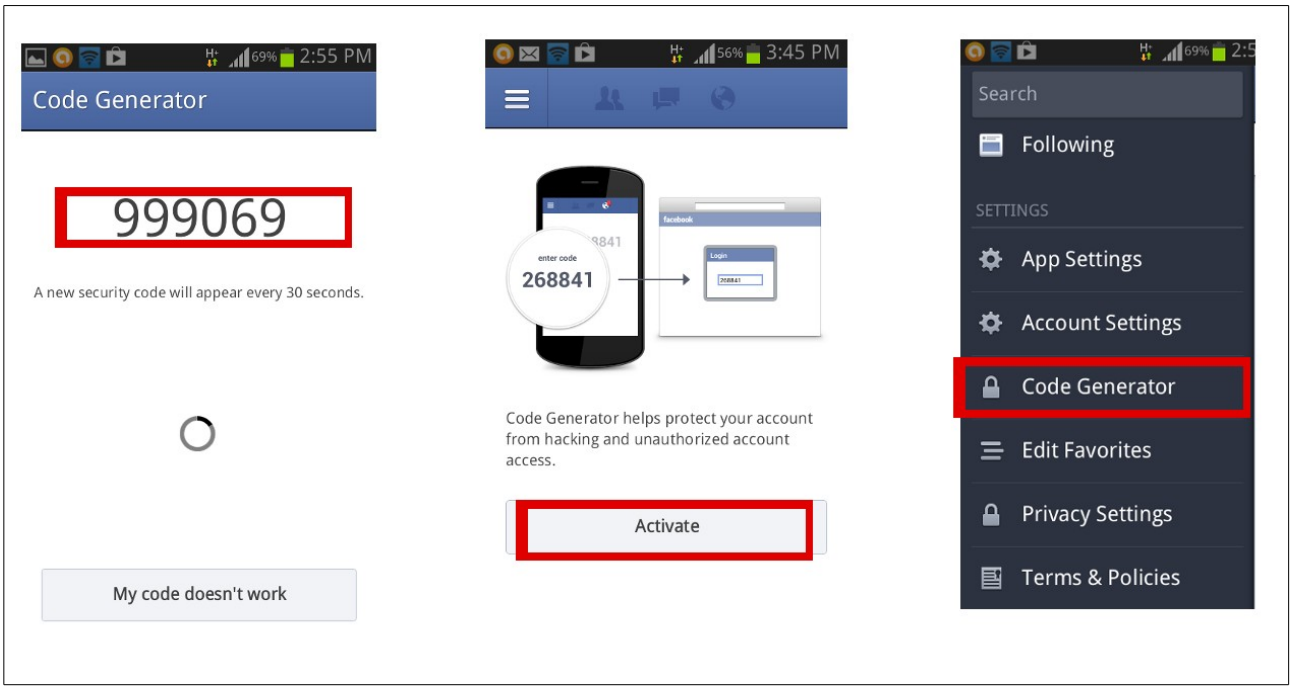
هذه الخاصية توفر لك خيارا هامة للأمان، حيث أنه في حالة محاولة أحد الولوج إلى حسابك على فيسبوك أو دخولك أنت من خلال متصفح أو هاتف محمول غير معروف، سيُطلب منه إدخال كود حماية، هذا الكود ستحصل عليه أنت من خلال تطبيق فيسبوك الموجود على هاتفك المحمول.



قم بتفعيل الخيار Login Approvals بالضغط على Require a security Code To access my Account From unknown browsers ، بعدها ستظهر نافذة جديدة تعطيك بعض المعلومات حول الخاصية، في أسفلها زر Get Started للانتقال إلى تفعيل الخاصية.

الخطوة الأولى لتفعيل هذه الخاصية أن تقوم باختيار نوع الهاتف الذي تستخدمه، ثم اضغط على الزر continue ، بعدها ستظهر لك نافذة جديدة، تخبرك بخطوات تفعيل الخاصية على هاتفك المحمول (سنقوم في الخطوات القادمة بشرح تفعيل الخاصية على الهاتف المحمول وكيفية الحصول على كود)، قم بالضغط على الزر continue ، الآن ستظهر لك نافذة (اختبار الكود Test Code (generator ، والتي تطلب منك إدخال كود للاستمرار في تفعيل الخاصية ، الآن اترك هذه الصفحة ولا تغلقها واتجه إلى هاتفك المحمول، افتح تطبيق فيسبوك، وقم بتحديثه إلى آخر إصدار إذا لم يكن محدث.

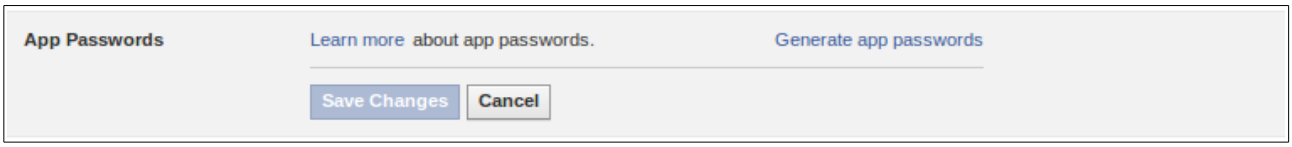
من تطبيق فيسبوك اختر Code Generator، بعدها سيطلب منك التطبيق تفعيل الخاصية، قم بالضغط على الزر Active بعدها سيظهر الكود كما في الصورة التالية:



هذا هو الكود الذي ستقوم باستخدامه للولوج إلى حاسب فيسبوك في حالة أنك قمت بالولوج من خلال متصفح أو هاتف غير معروف، ويجب أن تلاحظ أن هذا الكود غير صالح للاستخدام إلا خلال 30 ثانية فقط، بعدها يجب عليك الحصول على كود جديد.

الآن تبقي الخطوة الأخيرة، خذ الكود الذي حصلت عليه من تطبيق فيسبوك وقم بوضعه في نافذة اختبار الكود.

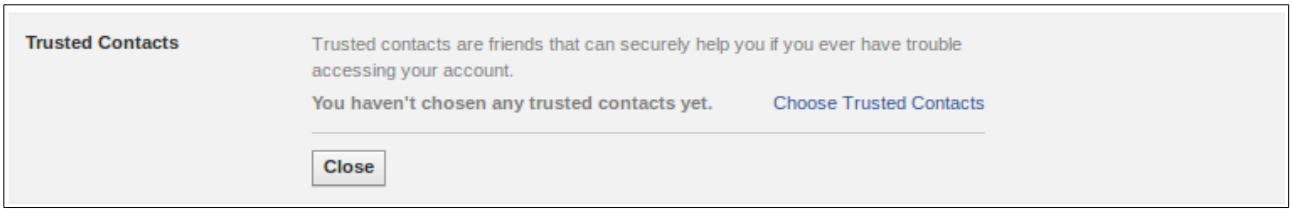
– App Passwords/كلمات سر التطبيقات



في حالة أنك تستخدم خاصية (Login Approvals/الموافقات على تسجيل الدخول) التي شرحناها مسبقا، ربما لن تستطيع استخدام حساب فيسبوك الخاص بك في بعض التطبيقات مثل Skype , jabber , Xbox لذلك خاصية **App Passwords/كلمات سر التطبيقات** توفر لك قدر عالي من الحماية بإمدادك بكلمات مرور مخصصة لهذه التطبيقات لاستخدامها بحرية والحفاظ على أمن معلومات حسابك، ولاستخدام هذه الخاصية بالضغط على Generate app Passwords، ستظهر لك نافذة قم بكتابة اسم للتطبيق الذي ستستخدمه ثم اضغط على زر Generate Password بعدها سيظهر لك كلمة المرور التي يمكنك استخدامها في التطبيق الذي تريده.

– Trusted Contacts/ جهات الاتصال الموثوق بها

هذه الخاصية توفر لك خيارا جديدا في حالة أن تم سرقة حسابك أو أنك نسيت كلمة المرور، حيث يمكنك اختيار 3 إلى 5 من أصدقائك الموثوق بهم يساعدونك لاحقا في حالة أنك لم تستطيع الدخول إلى حسابك.



لتفعيل الخاصية قم بالضغط على Choose Trusted Contacts وقم باختيار أي من أصدقائك على فيسبوك.

– Recognized Devices/ الأجهزة التي تم التعرف إليها

عند الدخول من أي متصفح أو هاتف محمول لحسابك على فيسبوك لأول مرة ستلاحظ أنه يُطلب منك الموافقة على تسجيل الدخول كما وضحنا في الخواص السابقة، خاصية (Recognized Devices/ الأجهزة التي تم التعرف إليها) توضح لك قائمة بالأجهزة والمتصفحات التي تستخدمها بشكل دائم مما يوفر عليك إزعاج تأكيد الموافقة على الدخول كل مرة تستخدم فيها أحد هذه المتصفحات.

– Active sessions / الجلسات النشطة

هذه الخاصية توفر لك معلومات حول الأجهزة التي قامت بالدخول إلى حسابك بفيسبوك مثل تاريخ الدخول إلى الحساب ونوع المتصفح ونظام التشغيل والمكان الذي تم الدخول منه، بالإضافة إلى الهواتف الذكية التي تم استخدام الحساب من خلالها

تويتر

في موقع التدوين المصغر تويتر لا يوجد خيارات متعددة للأمن والحماية كما في فيسبوك، وسنتناول بعض الخيارات المتاحة للحفاظ على حسابك بتويتر بالإضافة للنصائح العامة التي ذكرناها.

نصائح عامة

- **قم** باختيار كلمة مرور صعبه تحتوي على حروف صغيرة وكبيرة وأرقام ورموز، وحاول تغييرها على فترات لا تتجاوز ثلاثة أشهر.
- **كن** حذرا اتجاه التطبيقات التي تستخدمها على حساب تويتر، كتطبيقات الهواتف المحمولة أو تطبيقات الإنترنت التي تستخدم لإدارة الحساب، لا تستخدم إلا التطبيقات والمواقع الموثوق بها فقط، وراجع هذه التطبيقات كل فترة.
- **الروابط المختصرة** الموجودة في تغريدات المستخدمين تأكد من أنها لا تخفي خلفها روابط لصفحات ضارة ويمكنك أن تستخدم موقع http://longurl.org في معرفة الرابط الأصلي.

تجنب تتبع أعداد ضخمة من الحسابات ثم تقوم بإلغاء متابعتها وتكرار ذلك، أو استخدام المواقع التي تدعي أنها تزيد عدد متابعيك.

الرسائل المباشرة يمكنها أن تحتوي على روابط ضارة تطلب منك إدخال كلمة المرور واسم المستخدم، لا تقم أبدا باستخدام كلمة المرور واسم المستخدم في أي صفحة أو تطبيق غير موثوقة.

احمي بريدك الإلكتروني بقدر الإمكان، اختراق بريدك الإلكتروني يعني اختراق كافة حساباتك على الشبكات الاجتماعية.

– ربط الحساب برقم الهاتف المحمول

ربط حسابك بالهاتف المحمول يمكّنك لاحقا من استخدام خاصية "تأكيد الدخول/Login verification" حيث تتيح لك هذه الخاصية تأكيد الدخول إلى حسابك عبر كود يتم إرساله إلى رقم هاتفك المحمول، وسنتناول هذه الخاصية لاحقا.

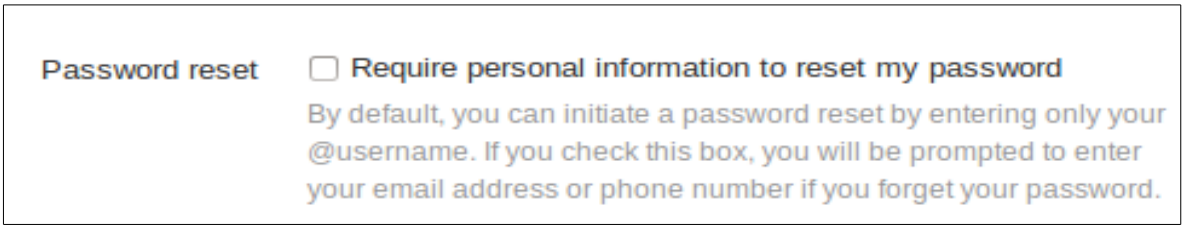
الآن لربط حسابك على تويتر برقم هاتفك المحمول ادخل إلى الإعدادات/ Settings، ثم قم باختيار التبويب Mobile /الهاتف المحمول من القائمة على الموجودة على اليسار، ستظهر لك صفحة تمكّنك من اختيار البلد ورقم الهاتف والشركة المقدمة لخدمة الاتصالات، قم بملأ الخانات ثم اضغط على الزر Activate phone بعدها ستصلك رسالة تأكيد على هاتفك المحمول.

– Password reset/إعادة تعيين كلمة المرور

في حالة أنك نسيت كلمة المرور الخاصة بحسابك على تويتر، سيُطلب منك أن تقوم إدخال اسم المستخدم على تويتر بعدها سيقوم تويتر بإرسال كلمة المرور إلى بريدك الإلكتروني.

تويتر يتيح لك خيارا أكثر أمانا لإعادة تعيين كلمة المرور الخاصة بك، حيث أنه في حالة طلب إعادة تعيين كلمة المرور لن يقوم تويتر فقط بطلب اسم المستخدم، لكن أيضا سيطلب البريد الإلكتروني أو رقم الهاتف المحمول.

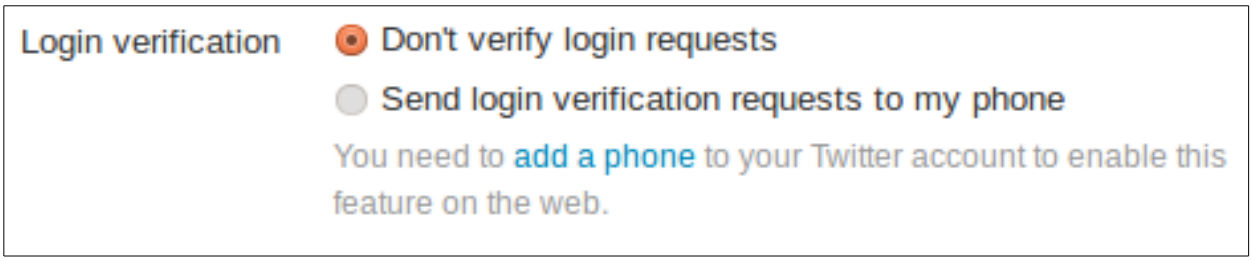
لتفعيل هذه الخاصية أدخل على التبويب Account من قائمة إعدادات تويتر Settings، ثم قم بتفعيل الخيار Password reset كما بالصورة التالية:



– Login verification

هذه الخاصية التي تحدثنا عليها مسبقا حيث تتيح لك تأكيد الدخول إلى حسابك عبر كود يتم إرساله إلى رقم هاتفك المحمول بحيث يطلب منك هذا الكود بعد إدخالك كلمة المرور الخاصة بك.

لتفعيل هذه الخاصية أدخل إلى التبويب account من قائمة إعدادات تويتر Settings، ثم قم بتفعيل الخيار Send login verification requests to my phone الموجود في الخاصية Login verification كما بالصورة التالية:



ملاحظة هامة:

استخدام هذه الخاصية غير متاحة للاستخدام في كل الدول، على سبيل المثال إذا كنت في مصر؛ ستكتشف أن تويتر لا يدعم إرسال رسائل قصيرة عبر الشركات المقدمة للخدمات الهاتف المحمول في مصر، لكن هناك طريقة أخرى لاستخدام هذه الخاصية عبر تطبيق تويتر للهواتف المحمولة.

– Login verification من خلال تطبيق تويتر على هاتفك المحمول

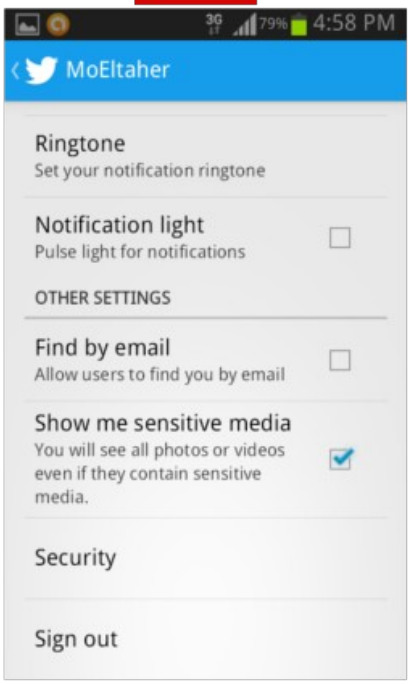
خاصية جديدة أضافها موقع (تويتر)مؤخرا، وتوفر هذه الخاصية إمكانية التأكد من هوية أي شخص يحاول الدخول إلى حساب تويتر الخاص عبر تطبيق تويتر الموجود بهاتفك المحمول، بحيث أنه عند طلب تسجيل الدخول على موقع تويتر، وبعد إدخال اسم المستخدم وكلمة المرور، يقوم الموقع بسؤالك عن (Back Up Code)، وهو الكود الذي يمكنك الحصول عليه من خلال تطبيق تويتر الموجود على هاتفك المحمول.

تفعيل واستخدام هذه الخدمة يعتمد بشكل أساسي على تطبيق تويتر الرسمي للهواتف الذكية، حيث أنه يمكنك تفعيله من من خيار security الموجود بإعدادات حسابك في تطبيق الهواتف الخاص بتويتر.

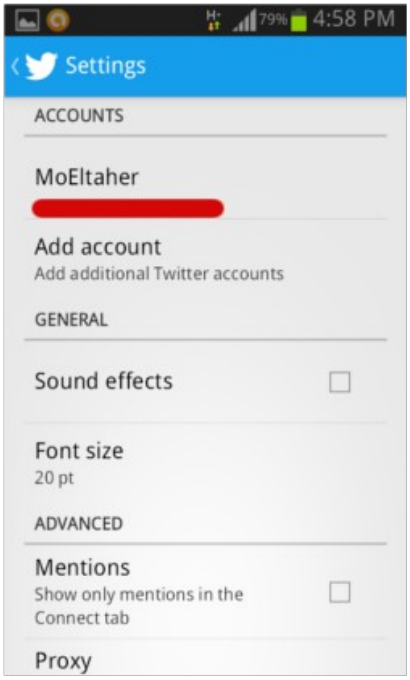
الآن لنقم بتفعيل وتشغيل الخدمة، **كما هو موضح في الصورة بأسفل:**

(1) افتح تطبيق تويتر من هاتفك، ثم قم بالذهاب إلى Settings ثم (2) إختر الحساب الذي تريد تفعيل هذه الخدمة فيه، (3) ومن القائمة التي تظهر لك ادخل إلى security الموجودة أسفل القائمة (4) قم بتفعيل خاصية Login verification كما موضح بالصورة (5) انتظر حتى يتم تفعيل الخاصية والحصول على الكود (Back up code)، بعدها (6) يظهر لك الكود وهو مكون من عدة حروف وأرقام.

3


4:58 PM
MoEltaher
Ringtone
Set your notification ringtone
Notification light
Pulse light for notifications
OTHER SETTINGS
Find by email
Allow users to find you by email
Show me sensitive media
You will see all photos or videos even if they contain sensitive media.
Security
Sign out

2


4:58 PM
Settings
ACCOUNTS
MoEltaher
Add account
Add additional Twitter accounts
GENERAL
Sound effects
Font size
20 pt
ADVANCED
Mentions
Show only mentions in the Connect tab
Proxy

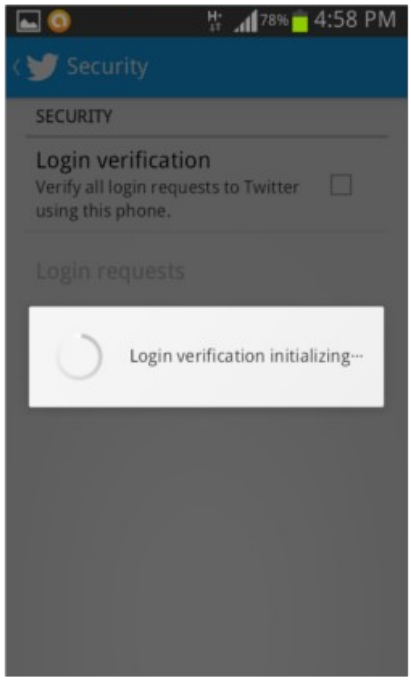
1


4:58 PM
Me
Mohamed El-Taher
@MoEltaher
10.4K
TWEETS
573
FOLLOWING
15.8K
FOLLOWERS
Mohamed El-Taher @··· 13h
Accounts
Settings
1d

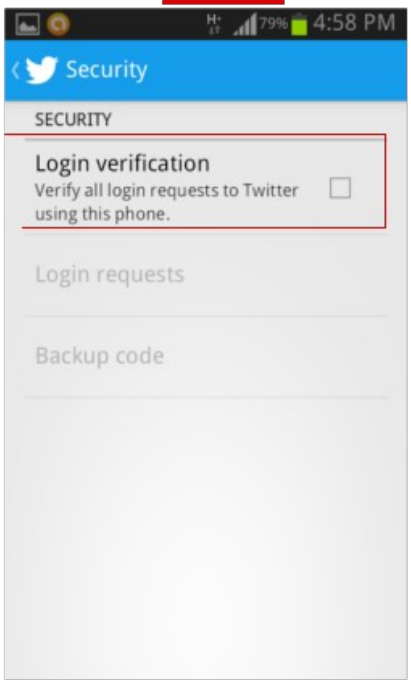
6


Saving screenshot···
Backup code
Generate new backup code
Write this down in case your phone is lost. You can also use a backup code when your phone is not connected to the internet.
Login verification enabled!

5

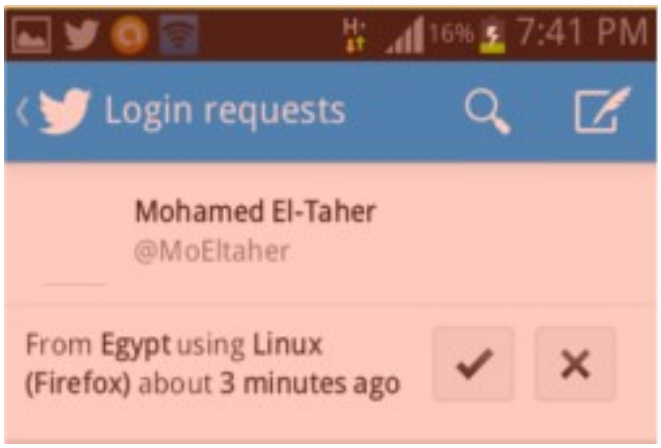

4:58 PM
Security
SECURITY
Login verification
Verify all login requests to Twitter using this phone.
Login requests
Login verification initializing···

4


4:58 PM
Security
SECURITY
Login verification
Verify all login requests to Twitter using this phone.
Login requests
Backup code

ملاحظة هامة: أنت في حاجة إلى الاحتفاظ بهذا الكود، حتى تستطيع أن تقوم بالدخول إلى حسابك في حالة إن فقدت هاتفك، لكنك لست بحاجة إلى إدخاله مع كل مرة تقوم بها بالولوج إلى حسابك، من حاسوب وهاتف ذكي جديدين، حيث يوفر التطبيق طريقة أخرى لاستكمال عملية تسجيل الدخول، بحيث تقوم أنت مباشرة بالموافقة على تسجيل الدخول لحسابك من خلال تطبيق تويتر على هاتف المحمول، وهذا ما سنتناوله في الجزئية القادمة

الآن قم بتجربة الدخول إلى تويتر، قم بوضع اسم المستخدم وكلمة المرور، واضغط sign in؛ ستلاحظ أن الموقع طلب منك إدخال back up code، وهنا أمامك خيران للاستمرار في تسجيل الدخول، **الأول** أن تقوم بالضغط على الزر backup code ثم إدخال الكود الموجود بالتطبيق تويتر على الهاتف كما وضحنا سابقا.



و **الثاني** أن تسمح بالدخول عبر التطبيق نفسه؛ وهذا يتم بفتح تطبيق تويتر على هاتفك المحمول ثم الذهاب إلى Security ثم الدخول إلى Login requests، ستلاحظ أن هناك (طلب) ظهر لك يطلب منك الموافقة/عدم الموافقة على الدخول إلى حسابك – كما بالصورة على اليسار- في حالة إنك كنت تريد السماح بالدخول قم بالضغط على (√) إذا كنت لا تريد ذلك اضغط على (X)، بعدها ستلاحظ أن صفحة الدخول المفتوحة على حاسبك انتقلت تلقائيا إلى الصفحة الرئيسية لتويتر وأنك قمت بالفعل بتسجيل الدخول بشكل صحيح.

Gmail

في الغالب عندما يحاول أحد اختراق حسابتك على مواقع الشبكات الاجتماعية يكون البريد الإلكتروني هو المنفذ لذلك، لهذا يجب الاهتمام جيدا إلى تأمين بريدك الإلكتروني بأقصى قدر ممكن.

هناك كثير من مقدمي خدمة البريد الإلكتروني المجاني، وقد تم اختيار Gmail لتناولة في هذا الدليل نظرا لأنه يحظي بشعبية واسعه، كما أن تأمينه يعني تأمين حساباتك الأخرى في خدمات جوجل، مثل يوتيوب وجوجل بلس.

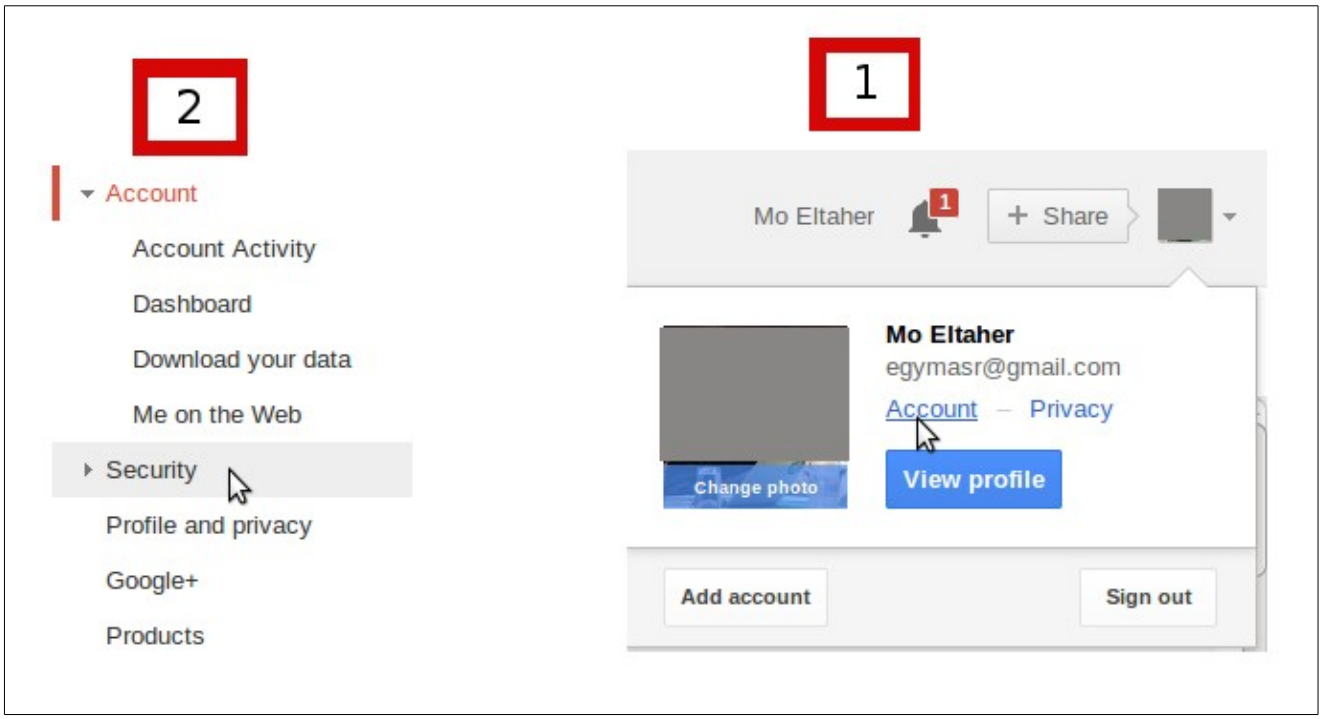
نصائح عامة

- **قم** باختيار كلمة مرور صعبة تحتوي على حروف صغيرة وكبيرة وأرقام ورموز، وحاول تغييرها على فترات لا تتجاوز أربعة أشهر.
- **تأكد** دائما أنك تستخدم خاصية SSL. يمكنك ذلك عن طريق تفعيلها دائما من خلال الذهاب إلى إعدادات البريد الإلكتروني: Settings > General > Browser Connection > check the "Always use https
- **اهتم** دائما بتحديث المتصفح الذي تستخدمه ويفضل استخدام Firefox
- **لا تستخدم** كلمة مرور البريد الإلكتروني ككلمة مرور في مواقع أو خدمات أخرى، لتكون في آمان أكثر في حالة اختراق هذه المواقع أو الخدمات.
- **استخدم** برامج مكافحة الفيروسات والجدران النارية وقم بتحديثهما باستمرار، ويفضل استخدام نظام تشغيل حر حيث أنه يوفر قدر عال من الحماية مثل توزيعات GNU/Linux
- **احمي** بريدك الإلكتروني بقدر الإمكان، اختراق بريدك الإلكتروني يعني اختراق كافة حساباتك على الشبكات الاجتماعية.
- **لا تقم** بتحميل أي ملفات مرفقة تأتيك من مصادر غير موثوق بها، وقم بفحص أي مرفقات ببرنامج لمكافحة الفيروسات بشكل إعتيادي.

جوجل يوفر عدد من خيارات الأمن والتي نتناولها في الجزء التالي:

– الدخول إلى إعدادات الأمن والحماية لـ Gmail

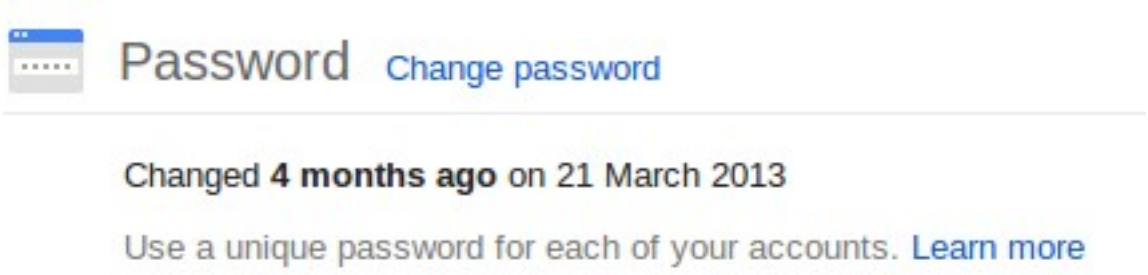
للدخول إلى إعداد الأمن الخاصة بحسابات جوجل، قم بالدخول إلى بريدك الإلكتروني ثم ادخل إلى Accounts ثم من القائمة الجانبية على اليسار إختر security ، كما موضح بالصورة التالية:



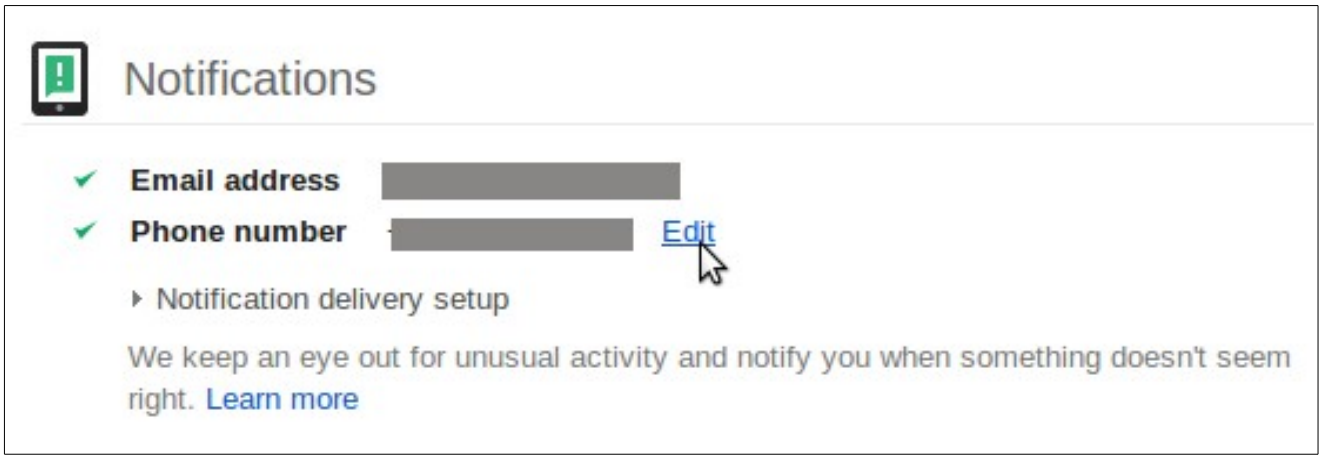
بعد الخطوات السابقة ستظهر لك مجموعة من خيارات الأمن والحماية سنتناول كل واحدة على حدة:

– Password/كلمة المرور

من هذا الخيار يمكنك تغيير كلمة المرور، ويفضل أن تقوم بتغييرها كل فترة (3-4 أشهر)، لتغيير كلمة المرور اضغط على Change password



– Recovery options/خيارات الاسترجاع



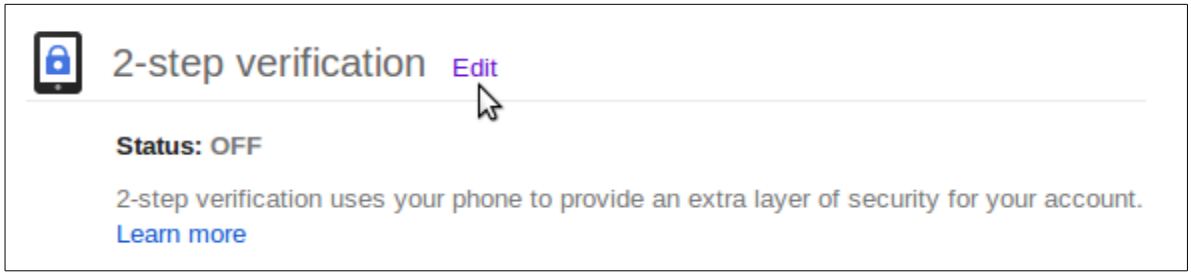
في حالة أن تم فقد البريد الإلكتروني الخاص بك، لأي سبب سواء نسيت كلمة المرور أو تم اختراقه، هذا الخيار يوفر لك طرق لاسترداد بريدك الإلكتروني، ويوجد طريقتين للاسترجاع، الأولي عبر البريد الإلكتروني والثانية عبر الهاتف المحمول، حيث في حالة فقدانك البريد الإلكتروني، يمكنك لجوجل أن تتأكد من هويتك عبر إرسال بريد إلكتروني، على البريد الإلكتروني الخاص بالاسترجاع Recovery email address أو البريد الإلكتروني البديل Alternate email addresses، أما الاسترجاع عبر الهاتف المحمول فيكون عبر التأكد من هويتك بإرسال رسالة نصية لرقم هاتف به كود تأكيد.

يمكنك تغيير أو إضافة رقم هاتفك والبريد الإلكتروني عبر الضغط على Edit والتي تنقلك لصفحة يمكنك من خلالها إضافة Mobile Phone و Recovery email address و Alternate email addresses ، ويفضل أن تقوم باستخدام الثلاث خيارات حتى توفر القد الأعلى من الحماية.

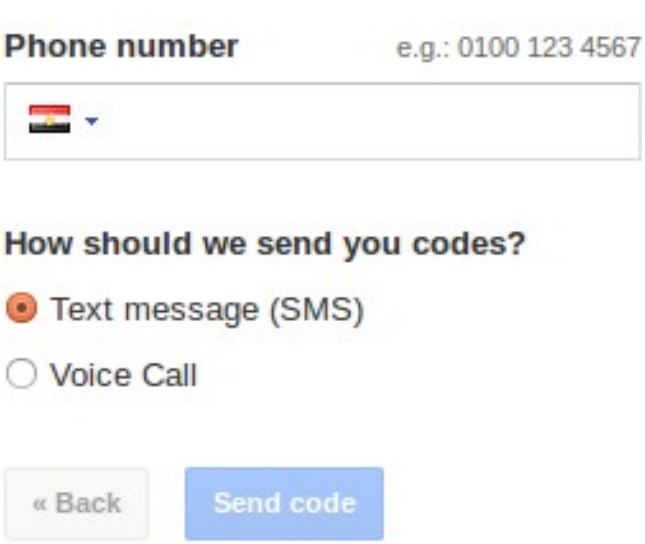
– step verification-2 /التحقق بخطوتين

في هذه الخاصية توفر جوجل خيارا إضافيا للدخول إلى حسابك، حيث أنه سيتطلب منك إدخال كود معين للسماح لك بدخول بريدك بجانب كلمة المستخدم.

لاستخدام هذه الخاصية اضغط على الزر Edit

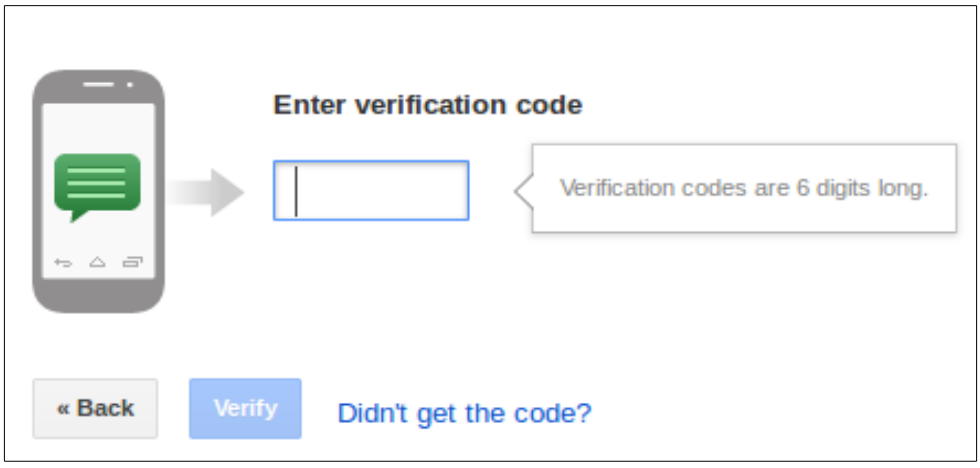


بعد الضغط على زر Edit ستظهر لك صفحة تطلب منك إدخال كلمة المرور والبريد الإلكتروني الخاص، قم بإدخالهما، تنتقل بعدها إلى صفحة تشرح لك الخاصية قم بالضغط على الزر Start set up، الآن نبدأ الإعداد.



الصفحة التي أمامك الآن تطلب منك اختيار الطريقة التي ستحصل من خلالها على الكود، هناك الخياران إما عن طريق الرسائل النصية القصيرة أو عن طريق خدمة google voice ، قم باختيار Text massage كما موضح بالصورة التالية، حيث أنها أسهر وأسرع في التعامل ومتوفرة للجميع.

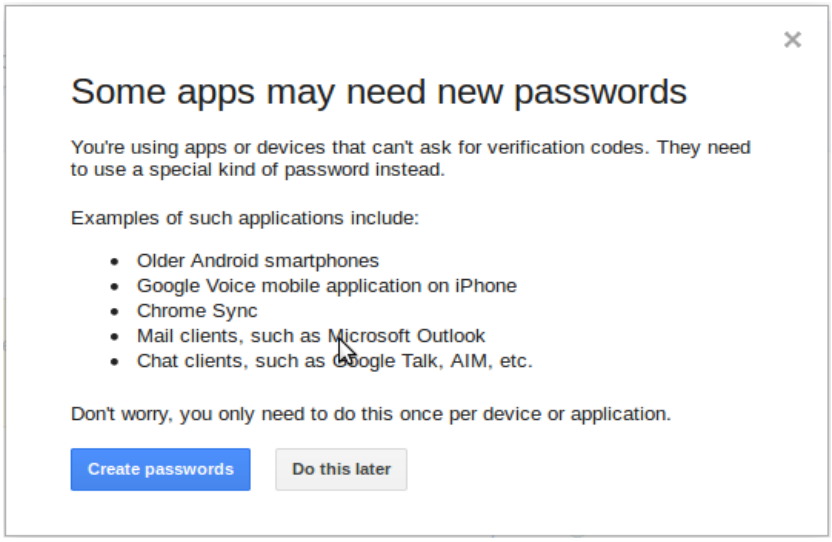
قم بإدخال رقم هاتف المحمول ثم اضغط على الزر Send code بعدها ستصلك رسالة على الهاتف المحمول الخاص بك بها كود التفعيل، كما أنك ستنتقل إلى صفحة جديد لإدخال هذا الكود، كما بالصورة التالية، ثم اضغط على الزر verify



بعدها ستنتقل إلى صفحة جديده تخبرك أنه تم التفعيل وتسأل ماذا كنت تريد أن تجعل الحاسب الذي تعمل من خلاله الآن حاسب موثوق به، بحيث تقوم بالدخول من خلاله إلى بريدك الإلكتروني منه دون الحاجة إلى التأكد كل مرة عن طريق إرسال كود إلى هاتفك، ينصح بهذا الخيار إذا كنت تعمل من حاسبك الشخصي وليس من مكان عام. الآن قم بالضغط على الزر Next للانتقال إلى الخطوة الأخرى.

بعد الضغط على الزر next ستظهر لك صفحة تُأكد لك أنه في حالة محاولتك الدخول إلى بريدك الإلكتروني في أي وقت ومن أي مكان سيتطلب منك كود التحقق في حالة أنك تدخل من حاسوب أو هاتف محمول غير معروف مسبقا، قم بالضغط على الزر Confirm للاستكمال.

بعد الضغط على الزر confirm تنتقل إلى صفحة جديدة -كما بالصورة-تخبرك أنه عليك الحصول على كلمات مرور لاستخدامها في التطبيقات والخدمات المرتبطة بالبريد الإلكتروني، على سبيل مثال ستحتاج إلى كلمة لاستخدامها في تطبيق البريد الإلكتروني على هاتفك المحمول أو الحاسوب الشخصي.

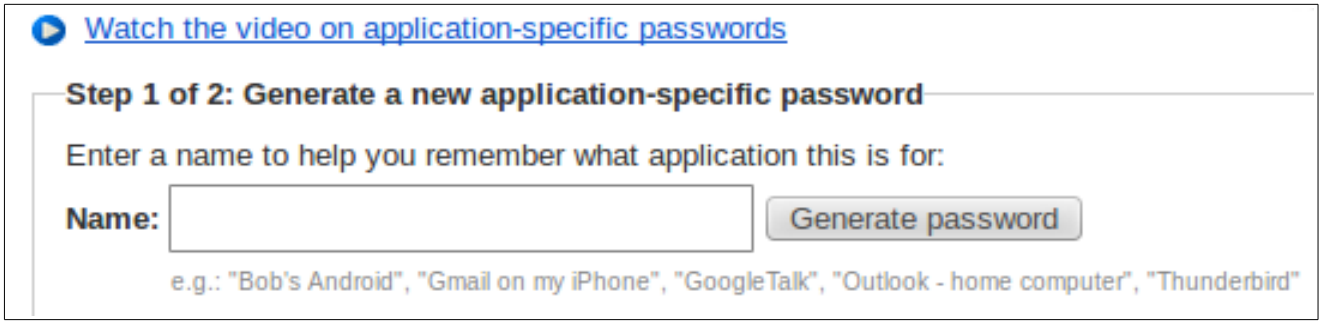


كلمات السر هذه ستستخدمها لأنك لن تستطيع استخدام الكود الذي تستخدمه في الولوج العادي لبريدك الإلكتروني، لذا يجب عليك أن تقوم باستخدام كلمات مرور مخصصة للتطبيقات.

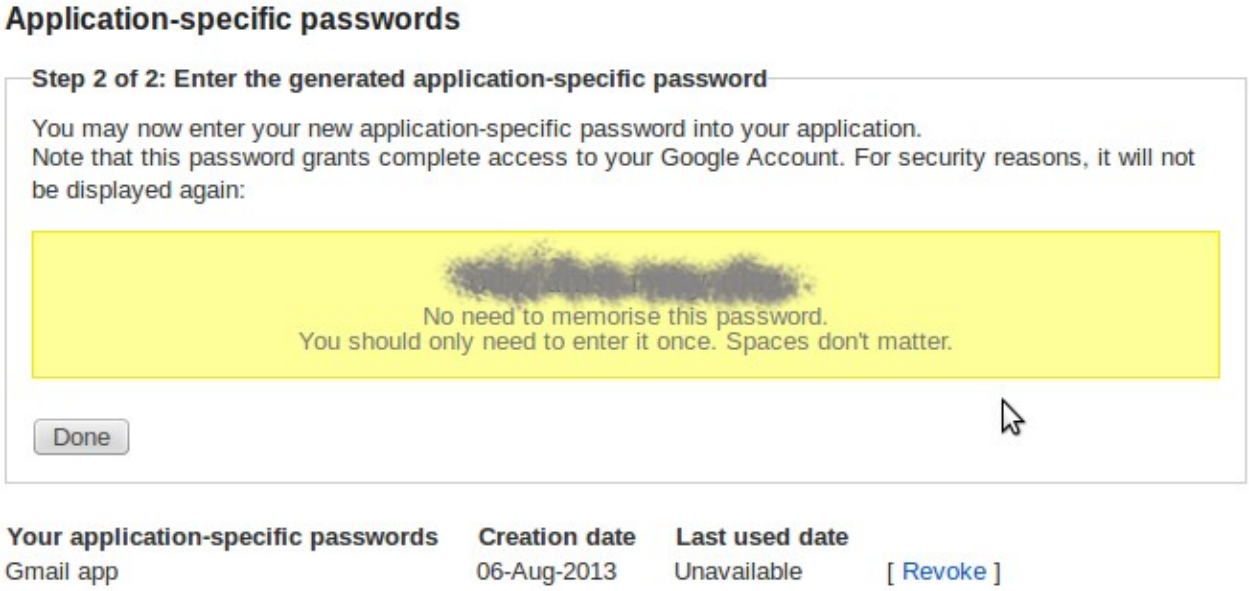
قم بالضغط على الزر create password بعدها تنتقل إلى صفحة جديدة تخبرك بأنه "ينصح بأخذ نسخه احتياطية من بريدك الإلكتروني" يمكنك تأجيل هذه الخطوة الآن والضغط على الزر remind me later.

بعدها تنتقل إلى صفحة "Authorised Access to your Google Account" وهي الصفحة التي تمكّنك من الحصول على كلمات مرور للتطبيقات التي تستخدمها.

كما بالصورة التالية قم كتابة اسم التطبيق، اختر أي اسم تريده على سبيل المثال "Gmail App" ثم اضغط على Generate password كما بالصورة التالية



الآن ستظهر لك كلمة مرور يمكنك استخدامها في أي تطبيق تريده كما بالصورة التالية



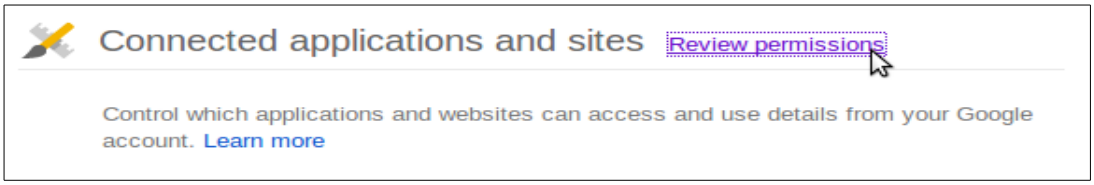
ملاحظة: لن تحتاج للاحتفاظ بكلمة المرور الخاصة بالتطبيقات، ستقوم بإدخاله لمرة واحده فقط ويمكنك الحصول على أكثر من كلمة مرور لكل التطبيقات التي تستخدمها.

هل يمكنني على الحصول على رموز التحقق بخطوتين بطريقة أخرى؟

نعم، إذا كنت تستخدم Android أو iPhone أو Blackberry يمكنك أن تقوم بتثبيت تطبيق Google Authenticator على هاتفك المحمول ومن خلاله تستطيع أن تقوم بإنشاء رموز التحقق بخطوتين حتى وإن كنت غير متصل بالإنترنت، لمعرفة كيفية استخدام هذا التطبيق اطلع على الجزء الخاص بـ(تثبيت أداة مصادقة Google) في مركز مساعدة حسابات جوجل عبر الرابط التالي:
https://support.google.com/accounts/answer/1066447?hl=ar

Connected applications and sites –

الخاصية الأخيرة هي Connected applications and sites وهذه الخاصة تتعلق بالتطبيقات والخدمات والمواقع التي تستخدم بريدك الإلكتروني للاتصال بها -مثل خدمة Feedly على سبيل المثال، وعند الضغط على Review permissions كما بالصورة التالية ستفتح لك صفحة جديدة يمكنك من خلالها أن تقوم بحذف الاتصال مع أي من الخدمات التي تستخدمها أو الحصول على كلمات مرور لاستخدامها مع هذه التطبيقات.



عن برنامج الحريات الرقمية

يعمل برنامج الحريات الرقمية بمؤسسة حرية الفكر والتعبير، على الدفاع عن حق الأفراد في الوصول إلى واستخدام وإنشاء ونشر محتوى رقمي، واستخدام أي حواسيب أو أجهزة إليكترونية، أو برمجيات أو شبكات اتصالات سلكية ولاسلكية.

ويأتي اهتمام مؤسسة حرية الفكر والتعبير بالحريات الرقمية، من ارتباطها بكثير من الحقوق والحريات الأخرى التي تدخل في نطاق اهتمام المؤسسة، كالحق في المعرفة وحرية الإعلام، وحرية الرأي والتعبير، والحريات الأكاديمية.

الأهداف العامة للبرنامج

إتاحة المعلومات حول الحقوق الرقمية

يعمل البرنامج على إتاحة المعلومات حول مفاهيم الحريات الرقمية ومبادئها، من خلال إصدار مواد مطبوعة أو تنظيم لقاءات عامة.

حماية الحريات والدعم القانوني

العمل على حماية حريات مستخدمي وسائل الاتصالات، مثل الحق في التعبير والحق في الخصوصية وحماية البيانات، وحرية تداول المعلومات، والعمل على وقف كل أشكال الرقابة أو الملاحقة الأمنية أو القانونية لأي من مستخدمي الإنترنت أو أي وسيلة اتصالات أخرى.

نشر ثقافة المصادر الحرة

يعمل البرنامج على نشر ثقافة المصادر الحرة في إنتاج المحتوى الإلكتروني أو البرمجيات، ورفع الوعي وتشجيع الاعتماد على رخص المصادر المفتوحة في النشر الإلكتروني بمختلف أنواعه.

تمكين الأفراد

يسعى البرنامج لتمكين الأفراد من حقوقهم الرقمية عبر الضغط لتحسين الجوانب السياسية والتشريعية المنظمة لقطاع الاتصالات وتكنولوجيا المعلومات في مصر.

إتاحة استخدام الطيف الترددي (الموجات الراديوية)

العمل على إطلاق حرية استخدام الموجات الراديوية، خاصة فيما يتعلق بإنشاء "راديو الهواة" وما يرتبط بها من حرية التعبير وحرية الإعلام، ودعم الإعلام المجتمعي والمحلي